Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue5,May-2017

Design And Implementation Of A Private And Public Key Crypto Processor And Its Application To A Security System

Shweta Madiwalar, Sandeep Kundargi, Chaya Bhat, Akshata Sangolli, Jyoti Sajjan

Electronics and Communication, KLE Dr.MSSCET
Telecommunication, KLE Dr.MSSCET
Telecommunication, KLE Dr.MSSCET
Telecommunication, KLE Dr.MSSCET
Telecommunication, KLE Dr.MSSCET

Abstract —This paper presents the design and implementation of a crypto processor, a special-purpose microprocessor optimized for the execution of cryptography algorithms. This crypto processor can be used for various security applications such as storage devices, embedded systems, network routers, security gateways using IPSec and SSL protocol, etc. The crypto processor consists of coprocessor blocks dedicated to the AES, triple-DES private key crypto algorithms and RSA public key crypto algorithm. The dedicated coprocessor block permits fast execution of encryption, decryption, and key scheduling operations. The crypto processor has been designed and implemented using an MATLAB.

Keywords- Encryption/ Decryption; Data Encryption Standard; Advanced Encryption Standard; RSA Algorithm; MATLAB; Public Key and Private Key.

I. INTRODUCTION

All companies, government agencies and home users depend on computer systems and communication systems such as the Internet and Intranet. The advent of computers and networks has completely changed the way in which we live and work. The expansion of the worldwide communication network such as the Internet and the increased dependency on digitized information in our society makes information more vulnerable to abuse. If there are security problems in these information systems, users will fear that their sensitive information may be monitored and business secrets stolen. For these reasons, it is important to make information systems secure by protecting data and resources from malicious acts crypto (cryptography) algorithms are the core of such security systems.

II. LITERATURE SURVEY

(1) Chandra M. Kota and CherifAissi, In this paper the implementation of the Rivest Shamir-Adleman (RSA) encryption algorithm is presented. The secret key consists of two large prime numbers p and q, and a part of the public key is their product, n = p*q. The RSA cryptosystem security is investigated.

(2) Chong Hee Kim, Differential fault analysis (DFA) finds the key of a block cipher using differential information between correct and faulty ciphertexts obtained by inducing faults during the computation of ciphertexts.

(3) Guang Gong and Solomon W. Golomb, The Data Encryption Standard (DES) can be regarded as a nonlinear feedback shift register (NLFSR) with input. From this point of view, the tools for pseudo-random sequence analysis are applied to the S-boxes in Data Encryption Standard (DES).

(4) HoWon Kim and Sunggu Lee,This paper presents the design and implementation of a crypto processor, a special-purpose microprocessor optimized for the execution of cryptography algorithms.

(5) Kun Ma, Han Liang, and Kaijie Wu, Fault-based attacks, which recover secret keys by deliberately introducing fault(s) in cipher implementations and analyzing the faulty outputs, have been proved to be extremely powerful.

(6) Salah Zaher, Amr Badr& Ibrahim Farag ,The problem of using RSA algorithm in cryptography is the long time it takes for the encryption process.

III. METHODOLOGY

3.1. Project Flow Chart

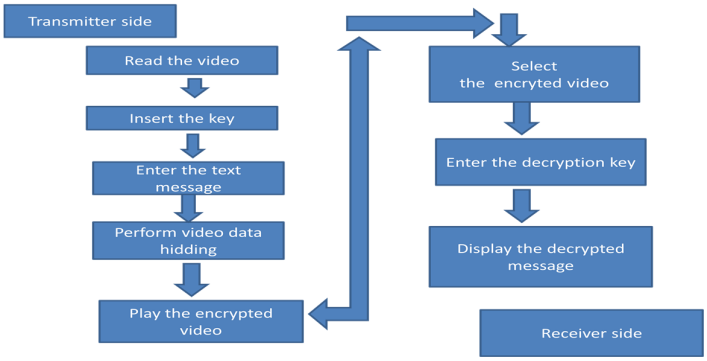

Figure 3.a. Flow Chart.

The model consists of Transmitter side and Receiver side. The transmitter side reads the video provided by the user and waits for the key insertion from the user. The text message needed to be encrypted is been entered which excepts it in ASCII value which is later converted to Hexadecimal format. The text is been encrypted and video hiding is been done in the selected video. At the Receiver side the Encrypted video is been selected ant then appropriate key is been entered for the decryption process. After successful decryption with correct key the original message is displayed as output.

3.1. The crypto-processor Architecture

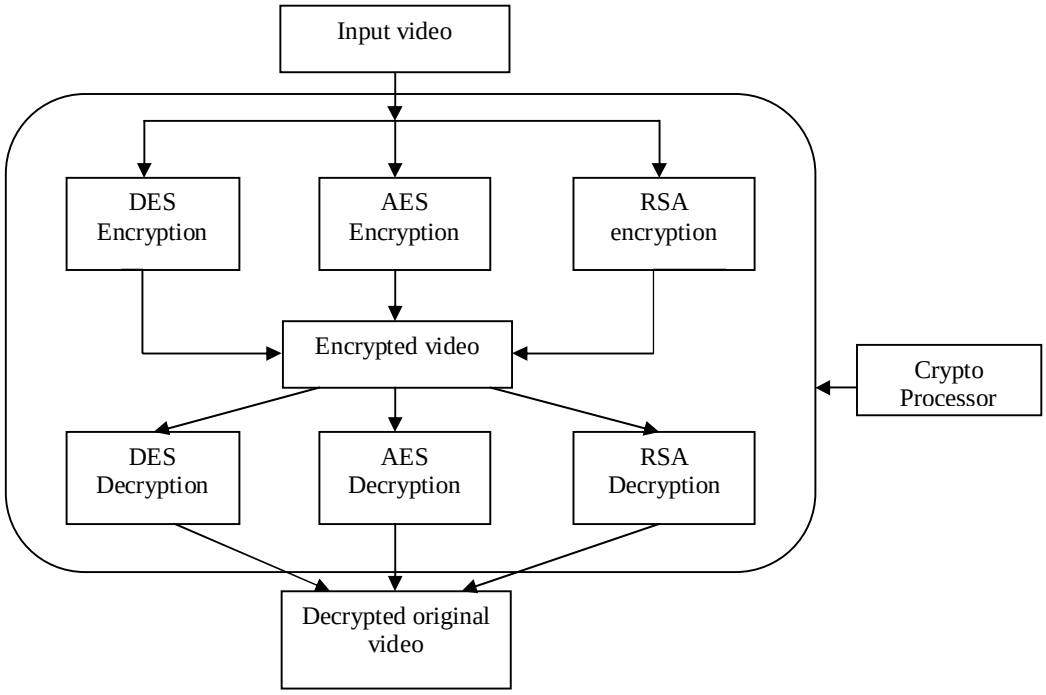

Figure 3.b. Block diagram of crypto processor

The crypto processor consists of three dedicated blocks for private and public key cryptography. Data encryption Standard and Advanced encryption Standard crypto blocks are used for Private Key encryption and RSA crypto block is used for Public Key cryptography. This crypto-processor can be interfaced with the 32-bit RISC type crypto controller that controls the dedicated crypto block and can perform the interface operations with external devices such as memory and an I/O bus interface controller. The dedicated crypto block results in fast execution of the encryption, decryption and key scheduling operations for the Advanced Encryption Standard (AES) and triple-Data Encryption Standard (DES) algorithms and enables fast scalar multiplication and exponentiation operations for the crypto algorithms.

3.2.Data Encryption Standard Crypto Block

Without doubt the first and the most significant modern symmetric encryption algorithm is the Data Encryption Standard (DES).The Data Encryption Standard (DES) was published by the United States National Bureau of Standards in January 1977 as an algorithm to be used for unclassified data (information not concerned with national security). The Data Encryption Standard (DES)is a block cipher operating on 64-bit data blocks.

The 16-round Feistel network, which constitutes the cryptographic core of Data Encryption Standard (DES), splits the 64- bit data blocks into two 32-bit words, LBlock and RBlock (denoted by L0 and R0). In each iteration (or round), the second word Ri is fed to a function f and the result is added to the first word Li. Then both words are swapped and the algorithm proceeds to the next iteration. The function f of Data Encryption Standard (DES) algorithm is key dependent and consists of 4 stages.

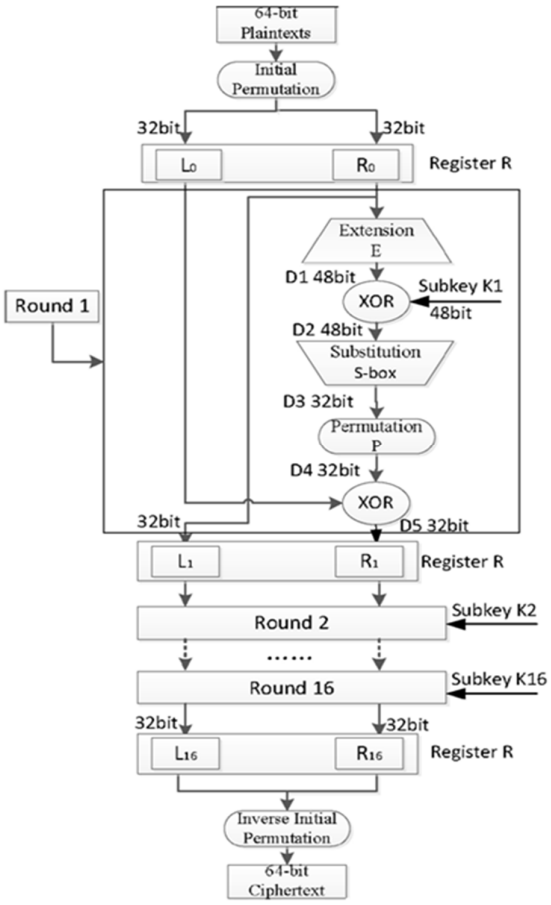

Figure 3.c. Data Encryption Standard Sequence

Data Encryption Standard (DES) (Data Encryption Standard) is a block cipher which uses a 64-bit key and operates on 64-bit blocks of data. Data Encryption Standard (DES) has a 56-bit key, because every 8th bit of the 64-bit key is used for parity checking The 56-bit key length is relatively small by today's standards. For increased security, the Data Encryption Standard (DES) operation can be performed three consecutive times, which expands the effective key length to 112 bits. Using Data Encryption Standard (DES) in this manner is referred to as triple-Data Encryption Standard (DES).

3.3.Key Schedule

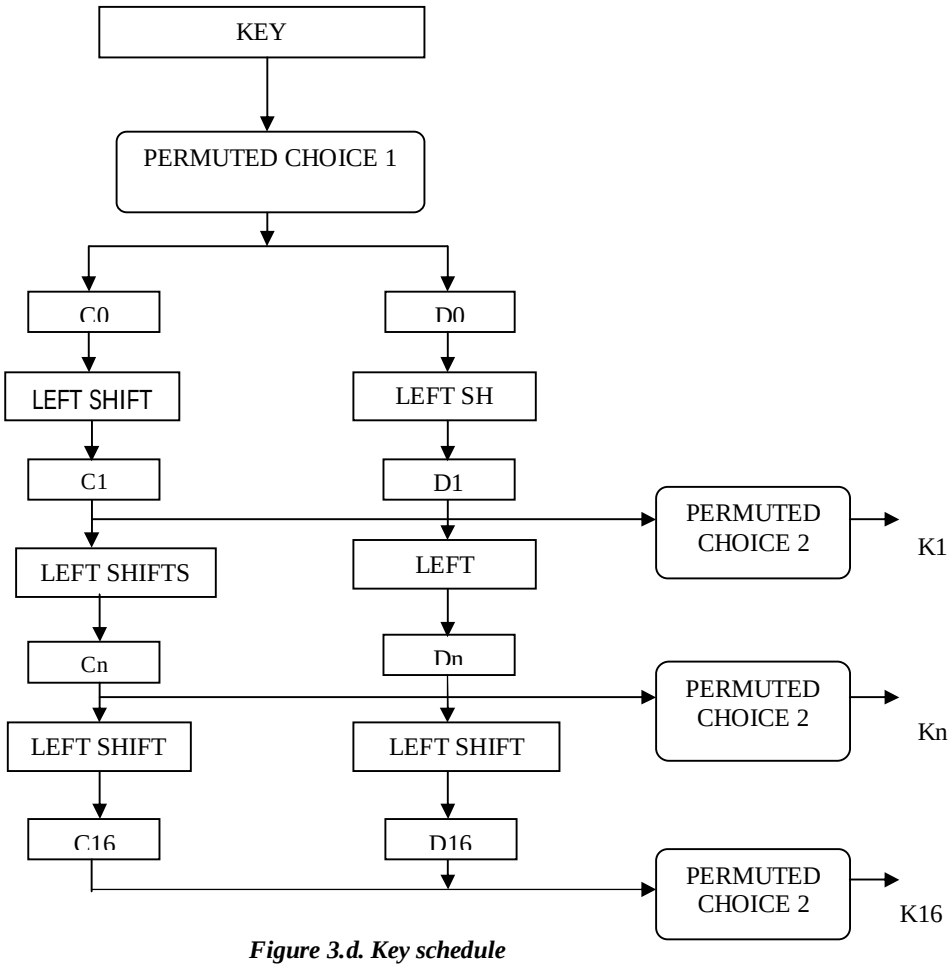

Figure 3.d. Key schedule

The first part of the table determines how the bits of C() are chosen, and the second part determines how the bits of D() are chosen. The bits of KEY are numbered 1 through 64. The bits of C () are respectively bits 57, 49, 41,..., 44 and 36 of KEY, with the bits of D() being bits 63, 55, 47,..., 12 and 4 of KEY. With C () and D () defined, we now define how the blocks Cn and Dn are obtained from the blocks Cn-1 and Dn-1, respectively, for n = 1, 2,….. 16.

IV. COMPARISION

The below Table 1 shows the comparative study between AES, DES and RSA into eighteen different factors associated and Table 2 briefs the Encryption and Decryption timings of AES,DES and RSA.

Table 1. Comparison between AES, DES and RSA

Factors	AES	DES	RSA
Developed	2000	1977	1978
Key Size	128, 192, 256 bits	56 bits	>1024 bits
Block Size	128 bits	64 bits	Minimum 512 bits
Ciphering & deciphering key	Same	Same	Different
Scalability	Not Scalable	It is scalable algorithm due to varying the key size and Block size.	Not Scalable
Algorithm	Symmetric Algorithm	Symmetric Algorithm	Asymmetric Algorithm

Encryption	Faster	Moderate	Slower
Decryption	Faster	Moderate	Slower
Power Consumption	Low	Low	High
Security	Excellent Secured	Not Secure Enough	Least Secure
Deposit of keys	Needed	Needed	Needed
Inherent Vulnerabilities	Brute Forced Attack	Brute Forced, Linear and differential cryptanalysis attack	Brute Forced and Oracle attack
Key Used	Same key used for Encrypt and Decrypt	Same key used for Encrypt and Decrypt	Different key used for Encrypt and Decrypt
Rounds	10/12/14	16	1
Stimulation Speed	Faster	Faster	Faster
Trojan Horse	Not proved	No	No
Hardware & Software Implementation	Faster	Better in hardware than in software	Not Efficient
Ciphering & Deciphering Algorithm	Different	Different	Same

Table 2.Comparisons of DES, AES and RSA of Encryption and Decryption Time

S.NO	Algorithm	Packet Size (KB)	Encryption Time (Sec)	Decryption Time (Sec)
1	AES	153	1.6	1
	DES		3.0	1.1
	RSA		7.3	4.9
2	AES	196	1.7	1.4
	DES		2.0	1.24
	RSA		8.5	5.9
3	AES	312	1.8	1.6
	DES		3.0	1.3
	RSA		7.8	5.1
4	AES	868	2.0	1.8
	DES		4.0	1.2
	RSA		8.2	5.1

V. CONCLUSION

In Data communication, encryption algorithm plays an important role. In this work different public and private key crypto algorithms have been studied and implemented in MATLAB on various images. These encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security. It is seen from the results that the decrypted image is same as input image in all algorithm techniques. It is found that the encryption/decryption of Advanced Encryption Standard (AES) algorithm is better than other algorithms. The simulation result shows that the evaluation of Advanced Encryption Standard (AES) algorithm is much better than Data Encryption Standard (DES) and RSA algorithm. The dedicated block of the crypto processor accelerates private and public key crypto algorithms and the programmability of the crypto controller results in fast execution of various security applications.

REFERENCES

[1] B.Scheier, "Applied Cryptography : Protocols, Algorithms and Source Code in C", 2nd ed.., John Wiley & Sons, 1995.

[2] Bruce Schneier, "*Applied cryptography(2nd ed.)"*, John Wiley and Sons, Inc., New York, 1996.

[3] Chandra M. Kota and Cherif Aissi, "Implementation of the RSA algorithm and its cryptanalysis", University of Louisiana at Lafayette, College of Engineering Lafayette, LA 70504, USA.

[4] Chong Hee Kim, "Improved Differential Fault Analysis on Advanced Encryption Standard (AES) Key Schedule", IEEE transactions on information forensics and security, vol. 7, no. 1, February 2012.

[5] Guang Gong and Solomon W. Golomb, "Transform Domain Analysis of Data Encryption Standard (DES)", Fellow, IEEE.

[6] HoWon Kimand Sunggu Lee, "Design and Implementation of a Private and Public Key Crypto Processor", Vol. 50, No. 1, FEBRUARY 2004.